

Ivanti Neurons for Secure Access

Descripción general

Ivanti Neurons for Secure Access ofrece gestión centralizada y análisis desde la nube para los gateways VPN Ivanti Connect Secure (ICS). Su interfaz unificada controla todo el despliegue de ICS, reduciendo enormemente el tiempo, la complejidad y los riesgos al administrar implementaciones VPN multinodo. El comportamiento de usuario riesgoso o anómalo se aborda mediante la remediación automatizada, mientras que los registros de gateway consolidados y los informes personalizables proporcionan información accionable. Neurons for Secure Access minimiza la carga operativa y mantiene un entorno seguro para maximizar el valor de su VPN.

¿Su despliegue VPN multinodo le está causando dolores de cabeza?

Con el auge del trabajo remoto, muchas organizaciones han ampliado significativamente su entorno VPN Ivanti Connect Secure para responder a la demanda de los usuarios en el Everywhere Workplace. Aunque una mayor conectividad es positiva para los usuarios, el aumento de la carga operativa para los administradores no lo es.

Los despliegues grandes pueden generar complejidad

A medida que su organización crece, necesita una forma de hacer más fácil, no más difícil, la gestión de todos sus gateways VPN. Necesita una herramienta para verificar, de un vistazo, que todos sus gateways estén en buen estado, actualizados y funcionando correctamente. También necesita una forma sencilla de aplicar cambios de configuración en todo el despliegue sin la molestia de iniciar sesión en varias interfaces, y necesita visibilidad sobre la actividad de todos los usuarios, sin importar cuándo o desde dónde se conecten a su red.

Señales de que necesita una mejor herramienta de gestión:

- Pasa horas cargando y desplegando la misma actualización en todos sus gateways VPN
- Un “cambio menor de configuración” lleva horas implementarlo en varias interfaces de gateway
- Su barra de favoritos del navegador está llena de páginas de acceso a gateways
- Recurre a su hoja de cálculo cada vez que le piden un informe de actividad VPN por regiones

Ivanti Neurons for Secure Access puede ayudarle

Ivanti Neurons for Secure Access soluciona el dolor de cabeza del VPN multinodo. Ya no tendrá que iniciar sesión en múltiples gateways para actualizar una sola política, combinar registros manualmente en una hoja de cálculo o cargar el mismo paquete de actualización en cada gateway individual. Neurons for Secure Access le proporciona gestión total de la configuración, administración completa del ciclo de vida de los gateways, actualizaciones con un solo clic, análisis del comportamiento del usuario, registros consolidados y herramientas de resolución de problemas, todo desde un gestor en la nube.

Cómo funciona

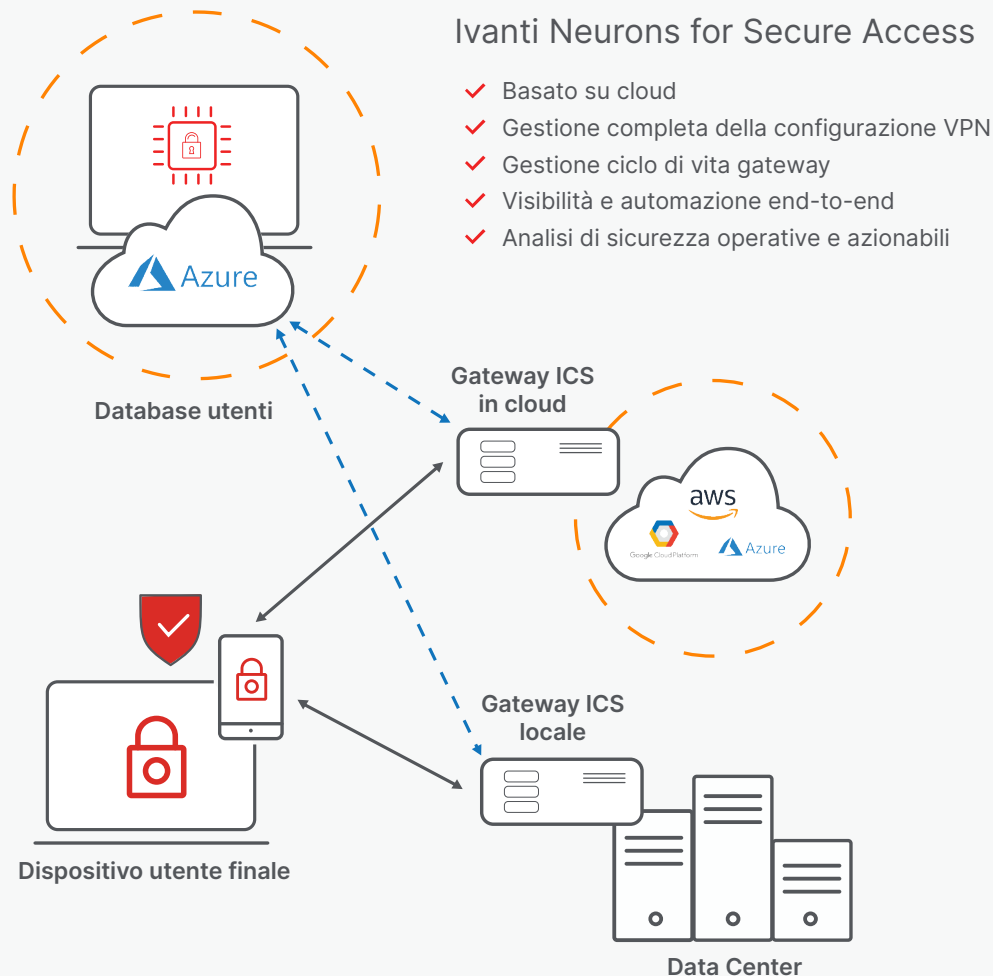
Ivanti Neurons for Secure Access es una plataforma centralizada de gestión y reporting SaaS para gateways VPN Ivanti Connect Secure (ICS). Proporciona una interfaz unificada que permite a los administradores de seguridad gestionar centralizadamente todos los despliegues de gateways ICS de forma rápida y eficiente.

Ivanti Neurons for Secure Access simplifica los flujos de trabajo y ahorra tiempo a los administradores mediante la consolidación de toda la configuración, registros, informes y datos de actividad de los gateways en un solo panel, eliminando la necesidad de hacer cambios en gateways individuales. Los administradores pueden replicar fácilmente configuraciones en varios gateways, lo que facilita la incorporación de nuevos gateways al entorno. La gestión del ciclo de vida permite actualizar o revertir gateways, clústeres o grupos de gateways en un solo clic, reduciendo considerablemente el tiempo y el esfuerzo necesarios para el despliegue de actualizaciones en todo el entorno VPN.

Los administradores también tienen acceso a herramientas de análisis y resolución de problemas para revisar el estado de seguridad y salud de toda la implementación VPN como parte de su rutina diaria. Con el Descubrimiento de Aplicaciones, pueden rastrear el acceso a aplicaciones través del VPN, visualizar métricas de uso y tendencias de acceso. Los informes programados permiten a los administradores diseñar, personalizar y automatizar reportes que reciben en su bandeja de entrada con los datos exactos que necesitan.

Neurons for Secure Access ofrece evaluación activa de riesgos de usuario mediante User Entity Behavioral Analytics (UEBA), donde se monitorizan y analizan los atributos de cada sesión VPN activa para detectar comportamientos riesgosos, sospechosos o anómalos, asignando un nivel de riesgo. Esta información permite a los administradores configurar la remediación automatizada del comportamiento de riesgo, como exigir autenticación secundaria o poner en cuarentena el cliente para una revisión adicional.

Neurons for Secure Access se aloja íntegramente en Microsoft Azure. No hay software ni appliances locales que instalar. Añadir un gateway VPN ICS a Neurons for Secure Access es tan simple como copiar un código de registro y una URL en el nuevo gateway y hacer clic en “unirse”.



Funcionalidad	Descripción
External Integrity Checker Tool (ICT)	<ul style="list-style-type: none"> ■ Análisis desde NSA a uno o múltiples gateways con un solo clic ■ Utilidad de seguridad diseñada para verificar la integridad de archivos y componentes críticos del sistema ■ Detecta cambios no autorizados, corrupción o manipulación ■ Ayuda a identificar posibles compromisos o anomalías comparando archivos con referencias validadas ■ Permite una respuesta más rápida a amenazas y mantiene la confiabilidad del sistema ■ Proporciona una alerta si se detecta una anomalía al ejecutar ICT en un gateway ■ Permite seleccionar un paquete ICT específico por versión, ejecutarlo sobre uno o múltiples gateways ICS y consultar los resultados en la misma página donde se ejecuta ICT
Gestión avanzada de licencias HTML5 Feature	<ul style="list-style-type: none"> ■ Permite a las organizaciones controlar y auditar tecnologías web disponibles para usuarios o desarrolladores ■ La gestión de licencias de funcionalidades HTML aporta beneficios de coste, legales, de seguridad y operativos
Secure Access Foundation	<ul style="list-style-type: none"> ■ Gestión completa de gateways VPN Ivanti Connect Secure ■ Visibilidad centralizada e informes de cumplimiento de usuarios, dispositivos, aplicaciones e infraestructura en toda la empresa ■ Alojado en la nube de Microsoft Azure sin software ni appliances locales que instalar ■ Actualice su infraestructura VPN a su propio ritmo
Gestión del ciclo de vida de Gateways	<ul style="list-style-type: none"> ■ Permite actualizaciones, regresos y reinicios centralizados ■ Experiencia de actualización "con un solo clic" ■ Soporte para actualizaciones de grupos y clústeres ■ Suite completa de herramientas de monitorización y resolución de problemas de nodos (ej. ping, traceroute, pcap, nslookup, instantáneas del sistema)
Gestión de Configuración	<ul style="list-style-type: none"> ■ Gestión centralizada y completa de la configuración de gateways ■ "Lift and shift" de configuraciones entre gateways mediante plantillas de configuración ■ Sincronización de configuraciones para gestión multinodo
Analítica del comportamiento de usuario (UEBA)	<ul style="list-style-type: none"> ■ Análisis propietario del comportamiento del usuario para identificar actividades riesgosas o anómalas ■ Automatización de respuestas ante niveles de riesgo elevados <ul style="list-style-type: none"> ■ Avisar al usuario por nivel de riesgo elevado ■ Forzar autenticación secundaria ■ Denegar próximos accesos con mensaje de advertencia ■ Desconectar/deshabilitar el acceso del usuario con advertencia

Funcionalidad	Descripción
Integración de servidor Syslog de nSA	<ul style="list-style-type: none"> ■ Permite la configuración de un servidor syslog externo para reenviar los logs del gateway ICS y los logs administrativos de inquilinos nSA ■ Ofrece gestión centralizada y segura de los registros y una mayor visibilidad del estado y eficiencia de los servicios que corren en los gateways ICS
Notificaciones de alertas offline	<ul style="list-style-type: none"> ■ El admin del tenant puede configurar alertas con direcciones de correo para definir destinatarios
Descubrimiento de aplicaciones	<ul style="list-style-type: none"> ■ Visibilidad de acceso a aplicaciones L3, L4 y L7 ■ Tendencias en el acceso a aplicaciones ■ Métricas de uso de aplicaciones
Reporting personalizado programado	<ul style="list-style-type: none"> ■ Creación de informes personalizados a partir de logs consolidados y envío por correo según agenda definida
Soporte de configuración híbrida	<ul style="list-style-type: none"> ■ Creación de informes personalizados a partir de logs consolidados y envío por correo según agenda definida ■ Soporta gateways VPN Ivanti Connect Secure físicos, virtuales o cloud ■ Soporta gateways VPN de la serie ISA de Ivanti ■ Coexiste con despliegues Ivanti Neurons for Zero Trust Access



Para más información o para contactar con Ivanti, visite [ivanti.com](https://www.ivanti.com).

Acerca de Ivanti

Ivanti es una empresa de software empresarial que proporciona una plataforma integral de TI y seguridad basada en la nube. Ivanti ofrece soluciones de software escalables alineadas con las necesidades de nuestros clientes para ayudar a TI y Seguridad a mejorar la eficiencia operativa, reducir costes y atajar proactivamente el riesgo de seguridad. La plataforma Ivanti Neurons es nativa cloud y está diseñada como el fundamento de servicios y herramientas unificadas y reutilizables para visibilidad consistente, escalabilidad y entrega segura de soluciones. Más de 34,000 clientes, incluyendo 85 de las empresas Fortune 100, han elegido Ivanti para afrontar retos con sus soluciones extremo a extremo. En Ivanti, nos esforzamos por crear un ambiente donde todas las perspectivas sean escuchadas, respetadas y valoradas, y estamos comprometidos con un futuro más sostenible para nuestros clientes, socios, empleados y el planeta. Para más información, visite [ivanti.com](https://www.ivanti.com) y síganos en @Golvanti.